ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol4, Issue 6, June 2017

Trust based Novel Secure Data Sharing Policy Framework for Social Networking

[1] Varun M Deshpande, [2] Dr Mydhili K. Nair
[1] PhD Student, Dept. of C.S.E., Jain University, Bangalore, India ,
[2] Professor, Dept. of I.S.E., M S Ramaiah Institute of Technology, Bangalore, India

***Abstract*— The advent of social networking and e-commerce empowered by cloud computing has created a paradigm shift in how people around the world communicate and do business. Amount of data being generated and information being shared by users is growing exponentially each hour. People around the world, have openly embraced the era of information technology, and almost unknowingly, it has become part and parcel of their daily life. However, the multitude of facilities provided by companies such as Facebook, Google, Amazon come with few potential concerns. Digital privacy of users and data security are at top of this list. Each company publish their own data policy and hence user generated data driven advertisements need to be analyzed carefully and holistic privacy preserving regulations enforced. We highlight results obtained from an online survey conducted to get an end-user perspective to these concerns on their digital identity. A compulsive effort is required to setup open standards based policy framework to achieve privacy preserving social networking and secure opt out mechanism needs to be offered to the users who do not wish to share their personal details with 3 rd party. We describe a trust based novel secure data sharing framework for implementing open standards on data security and privacy. This would be one step towards providing trustable software solutions for secure cloud based services.**

***Keywords*: Privacy, policy, data security, digital identity, open standards, privacy framework, trust**

I. INTRODUCTION

A. Cloud Computing-definitions

Cloud computing refers to all computer based applications and services that run on highly distributed network leveraging on virtualization technology. These services can be accessed by computing devices for communications. This virtual setup gives an illusion of limitless resources and totally abstracts physical machines where computation happens from the end user of the system. The U.S. National Institute of Standards and Technology (NIST) provides a set of working definitions for cloud. Per them (figure 1), cloud model consists of 5 essential characteristics or service attributes: Resource pooling, broad network access, measured service, on-demand self- service, and rapid elasticity. Cloud service models define what the different types of services provided are. There are mainly 3 service models defined: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). While deployment models are Public, Private, Hybrid and Community [1], [2].

B. SaaS Services

Gartner defines cloud computing as ―a style of computing in which scalable and elastic IT-enabled capabilities are delivered as a service using Internet technologies‖. This definition gives an overview of cloud service models offered by cloud platform. In the current study, we are dealing especially with SaaS model. In this model a complete end-to- end service is hosted by the service provider and the end user is given a simple client interface such as a desktop/mobile application or a browser to access the services. Some examples that come under this service model are social networking websites such as Facebook, Google Plus. Social networking has reunited countless friends and families who were separated by time and space. They include e- mail/messenger service providers such as Google, Yahoo. Email services help us to send and receive mails to and from anyone in the world via our email id. They also include e- commerce websites such as Amazon, Flipkart. E-commerce websites have changed the way people shop and sell.

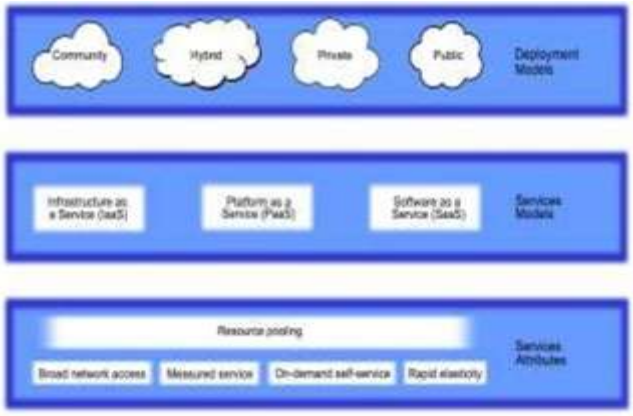


Figure 1: NIST definitions for cloud

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol4, Issue 6, June 2017

II.RESEARCH DOMAIN

A. Why we should worry?

In many instances, SaaS service providers provide service to end users at free of cost to attract more number of users of the service. Social networking companies and email service providers rely hugely on personalized advertisements to monetize. Google reported revenue of $24.7 Billion and Facebook reported $8.03 Billion in Q1 2017 which rely heavily on advertising (publicly available information). This is how they can sustain and make profit of a free service that they provide to millions of customers online who use their services extensively. For example, Google and Facebook has close to 2 Billion monthly active users. E-commerce websites make their earnings from commission it gets when an online purchase is made using their platform. As commission, may be less, they rely heavily on high volume of sales. In any case, service providers who provide free SaaS services have a lot riding upon the number of users using their platform. Also, the amount of information that is being shared, content created or amount of business transactions that happen online via their services have impact on their revenue.

At the outset, this model seems to be perfectly blending into a win-win relationship between service provider and end user. End users get world class services at absolute free of cost. Whereas service providers make profit using advertisements. The usage of service is bounded by terms of service. End users tend to trust the service provider with their information and believe that it is safe in their hands. However, Chi Zhang et. al.[3] note that online social networking websites raise issue of privacy and data security. In their work, they discussed about design issues for security and privacy of social networks. They note that there were several design conflicts when it came to achieving goals such as privacy preserving data mining capabilities. Data mining and data privacy are tough to blend with each other as one relies on tradeoffs on privacy to achieve meaningful results and still research work is required there. They conclude by saying experts from social science, security companies and other regulatory bodies need to come together and collaborate to build secure privacy preserving mechanisms. Current work is a step towards this research direction. Cutillo et. al.[4] mark that exponential growth in usage of social networking sites have raised serious concerns about privacy and security. They note that along with existing security risks which are associated with cloud, specific issue pertaining to privacy is highlighted as they are dealing with personal data of end users. Dwyer et. al. [5] did a comparison of privacy concern and its relation with trust influence. Their study concentrated on users of Facebook and MySpace. They dwelled into behavioral aspects of people using the websites. Per them, there is still a lot of work to be done in this space as trust and privacy concerns in social networking was still not understood completely. Hence addressing digital privacy and data security issues remains very relevant and important topic today.

B. Online Survey on Digital Privacy and Data Security

As a first step, we tried to understand an end user's perspective of what digital privacy means to them. We listed some of the basic questions that concern us as day to day users of SaaS services. We then prepared a scientific questioner which was unbiased and precise. It gave users enough choices for answering. For each question, they had an option to write their own answer if they felt options didn't fit their thought process. We conducted a survey of cyber literate people contacting them via different SaaS services like Google, Facebook, Whatsapp etc. In a short background of survey was given to set the context – ―This survey is part of academic research work for review of practical concerns faced by users regarding digital privacy and data security in cloud - social networks/ mail service providers etc.‖ We got responses from 114 people over a period of 1 month [15]. Among the respondents, 29% were women and remaining
71% were male. From age distribution of participants, it was notable that more than half the respondents were of age category 26-35 and age category 21-25 was next to follow. We did get representations from other age categories as well. Their profession grouping was also recorded. People from Corporate sector were a clear majority among respondents. It was also noted that 95% of the total respondents were daily users of at least one of SaaS services.

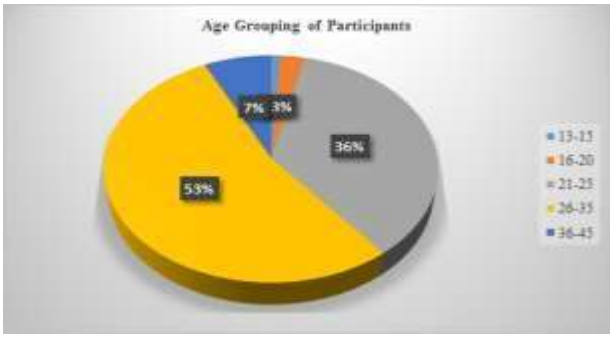


Figure 2: Age grouping of respondents

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol4, Issue 6, June 2017

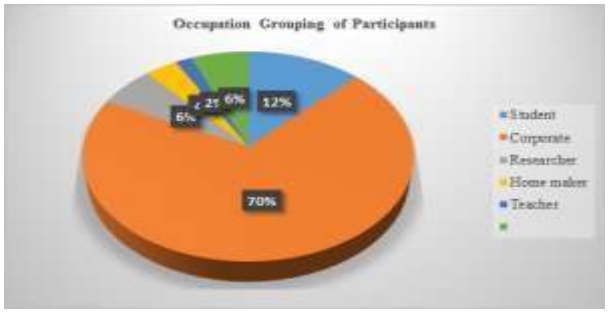


Figure 3: Profession grouping of respondents

As a small social experiment, we kept 2 optional questions pertaining to personal information to record the willingness of people to share their information with surveyor. ―Name‖ was one of them. Surprisingly, 89% of people provided their name even though it was not required for them to do so. While there were 11% of people who refrained from disclosing their name for the research. ―Name‖ is such an attribute which can't help in identifying a person's identity on its own. But it can help in short listing candidate matches and increase chances to identifying person combining with some other available data such as age group and profession. In the question related to emails, we said that we would be emailing a copy of gathered research data if they wished to be notified about the same. An email-id can act as an identifier if someone is trying to identify the person. Here we found that about 58% of respondents did provide their email-id with hope that they would be benefitted by analyzing research survey results. This mini-experiment was solely for research work and we have made sure that none of the names or the email-id have been disclosed while publishing survey results. It is just a testament to our observation that people may be tricked into sharing information about themselves in some or the other way which may come back and haunt them later.

We asked a total of 9 questions relating to digital privacy and data security. All questions were having multiple choice and had option for entering their own answer if they wished to. 1st question was ―How much thought do you give when you share personal information with public on any social network?" As a supplement to question, we gave the context of given question- ―Personal information can be like Mobile number, Street address, Credit card etc.‖ Total of 62% of the respondents said that they shared their personal information only when they felt it was necessary for them to do so. While

33% of them said that they never shared such information publicly. Whereas small number of users were indifferent about it. However, these are the same respondents who shared

their names when it was not required. It shows that though users are cautious about sharing personal information, they may be sharing information without their knowledge or not expecting any adverse effects in doing so.

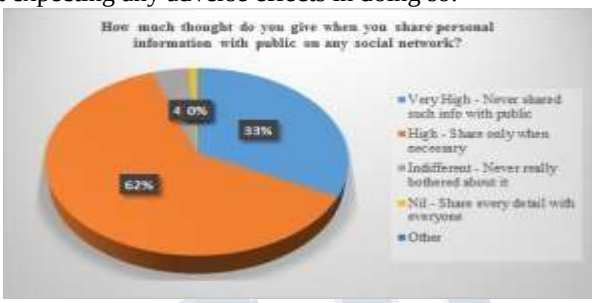


Figure 4: Question 1

In 2nd question, we asked ―Advertisements provided by service provider based on your online activity is cause of concern to you?" and as a context, ―Are you concerned about being snooped upon when you see an advert matching your online activity or is it pretty convenient‖ For this question we got varied responses. More than half of respondents expressed that they very concerned about seeing advertisements based on their online activity and even felt that it may be breach of privacy. While one third of them were empathetic towards service providers and felt that it was how service providers could sustain the services that they are providing to end users. About 10% felt that they were benefitted by the advertisements and that it was a win-win situation for them and the service provider. This question raises interesting question about what are the set of personal information that is being used to find suitable advertisements for the individual.

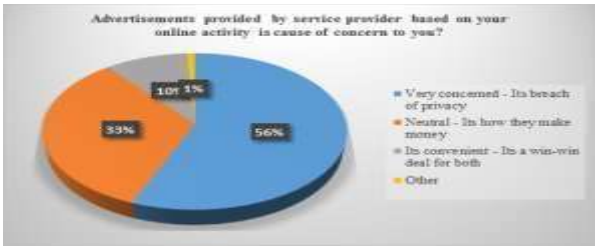


Figure 5: Question 2

3rd

question that we asked was – ―How much confidence do you have about your data available in service provider's website is safe?‖ and as a context, ―Are you comfortable knowing that service providers are owning your data?‖ This question was asked to understand the level of

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol4, Issue 6, June 2017

trust that people have on service providers. 37% of respondents expressed that they were highly concerned about the service provider's website and data security. While 55% were cautiously concerned about data security and felt that if they are following protocols, it should be fine. There were few respondents who were either indifferent to it or not concerned about it at all. This directs our attention to the existing policies & regulations and need to revisit them and make it as transparent as possible.

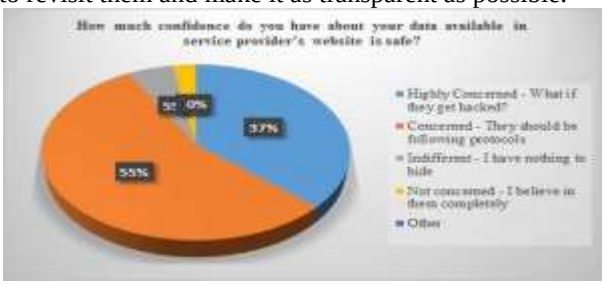


Figure 6: Question 3

In 4th question we asked- ―Do you feel that your online activity has effect on your digital identity?‖ and context was- ―As your online activity decides the content you see; do you feel it has a say on decisions you take.‖ This question was asked specifically to know respondent's view on their digital identity and how it was getting affected by their online activity. Half the people felt that, their online activity such as liking a post or sharing certain video, surfing for certain product, being friend with certain person etc. has had sub conscious effect on their digital identity and influenced how they felt they were being perceived by others. While one third of respondents were of strong opinion that it has direct effect on their digital identity. There were still about 17% of respondents who thought that they were either indifferent or that it helped in building their digital identity.

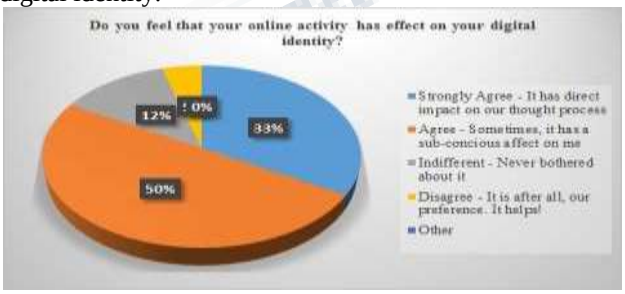


Figure 7: Question 4

In 5th question we asked-―Do you have concern that your information may be sold to any 3rd party?" and as a context, ―As a user, do you feel that you have control over your data?‖ Although it may seem as a biased question, we felt that it was necessary to ask about this as it has affected so many people in world. Close to half the respondents were highly concerned about their Personally Identifiable Information (PII) being shared/sold with/to 3rd party. 39% were concerned about it and they expressed concern over sales calls that they get from companies they never heard of before. This may be extended to emails or even postal messages. More than 10% were not bothered about such things and a small fraction of people completely trusted their service provider and believed that their information is safe with them. Again, this directs us to understand further into terms of data disclosures and kind of anonymization algorithms that are being used there.

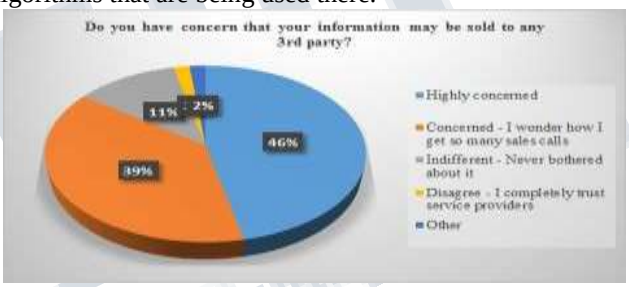
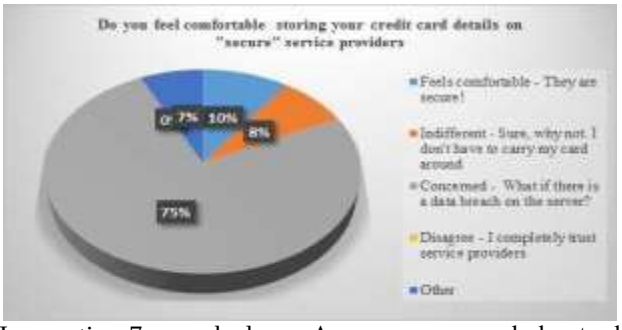


Figure 8: Question 5

In question 6, we asked –―Do you feel comfortable storing your credit card details on "secure" service providers" and as a context, ―For convenience sake, do you feel it is okay to save your financial data online?‖ Although this question is concerned with people who use credit/debit cards for online transactions, we felt this is a very relevant question in the context of research work as it is an indicator of level of trust in return for convenience of usage. Surprisingly, we got a polarized result for this question as 75% of people were concerned about storing financially critical data online on trusted servers. The concern is: what If there was a data breach on the server. About 10% of people were comfortable enough in storing their financial data online. Soft data is such an entity that it is very hard to get to know if or who made a copy of it and when. This is because original data still exists in the same place. This is fundamental difference between stealing soft data and hard copy of some documents for example. Hence this becomes very important for researchers to ensure that they stay ahead and out-wit the hackers who are on a constant look out for people's financial data

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol4, Issue 6, June 2017



In question 7 we asked – ―Are you concerned about what happens to your existing data if you wish to stop using a service‖ and as a context, ―Do you feel that your data would be safely destroyed once you wish to exit using the service?‖ We felt that this question is very necessary as most people might not have even asked this question to themselves. 32% expressed that they were highly concerned about data deletion policies and wondered if their data trail would ever be deleted. Closed to 60% of people concerned about the data deletion policies and they did not know what the associated rules were for this. There were about 9% of people who were indifferent to data deletion policies. We feel that this is one of the key research areas as we need to understand clearly what happens when user wishes to terminate his usage of service and how his/her data is handled.

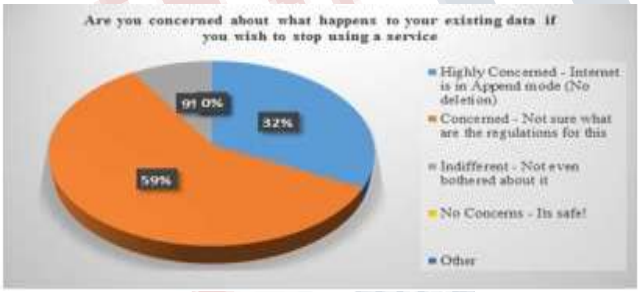
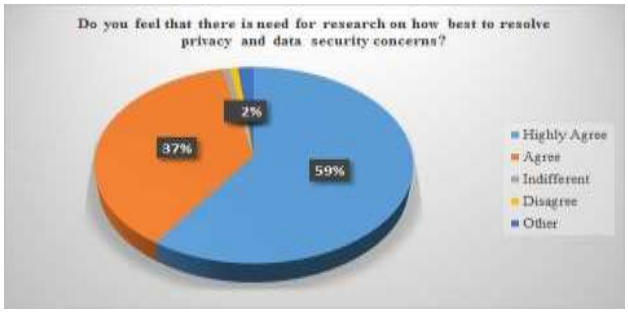


Figure 10: Question 7

In question 8, we asked – ―Do you feel that there is need for research on how best to resolve privacy and data security concerns?‖ and context was ―Cloud - Social networks/ Mail Services/ E-commerce sites are making our life so much easy! But they come with their baggage too. Do you feel further research is needed in this domain?‖ 59% of the respondents strongly agreed that there is a need for more research in this field. While 37% said that they agreed that it was an important research area.



In 9th question, we asked "Do you feel users should be able to fully control about what data is shared with whom?" and context was ―Though website is owned by service providers, do you think there is a need for more comprehensive user driven privacy and security settings‖ This question was asked to get a know if people care about having control of their data hosted on service provider's web space. Close to 70% of people strongly agreed while most of others agreed that it was important to consider the same.

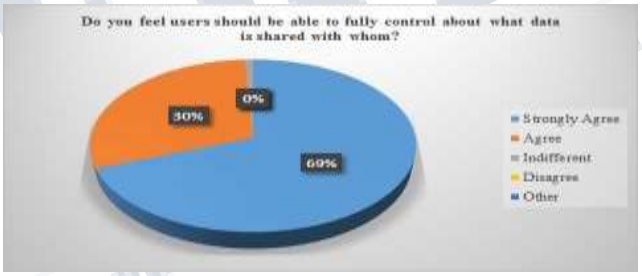


Figure 12: Question 9

With these questions, we covered several of privacy and data security related research questions and got inputs from an end user's perspective. This will help us in identifying key areas of research and direction to proceed further. Most of the respondents were Indians.

III.REVIEW OF LITERATURE

In this section, we have highlighted some of the existing work that has been done in the research domain. This helps us in understanding existing concerns and solutions. Also, it helps in identifying areas where we need to put our efforts on.

Data mining deals with extracting useful information and trends from multitude of available data. However, concern arises when the data contains information related to PII of individuals or group of individuals. Some of the data anonymization techniques currently in practice are ―k-anonymity‖, ―I-diversity and t-closeness‖, ―Differential

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol4, Issue 6, June 2017

Privacy‖ [6]. They also mark that publishing complex network data with privacy guarantees remains a challenge and developing rigorous privacy definitions to address growing complexity of network data is a very important research direction.

With growing popularity of social networking sites people are sharing lot of information about themselves online leaving a long trail of PIIs. This obviously possess serious threats of user privacy. G. Brown et. al.[7] documented some of the most common privacy threats. They include identity theft, digital stalking, and personalized spam. There have been several incidents especially in recent years where privacy breach has caused irreversible damages to an individual or a family.

Elena Zheleva[6] defines that ―privacy breach occurs when a piece of sensitive information about an individual is disclosed to an adversary, someone whose goal is to access information that they are not authorized to access.‖ They discuss four different types of privacy breaches including identity disclosure and attribute disclosure. They also discuss about social link disclosure and affiliation link disclosure which are specifically concerned with social networking websites.

In 2014, Facebook bought Whatsapp for an amount of $19 Billion. Number of active Whatsapp users were estimated around 450 Million at that time. This meant that Facebook paid about $42.2 for each person who used Whatsapp which does not even sell advertisements in their application as of now. This only shows how importance of customer reach and user's data to companies. This puts question #9 of the survey in perspective and there should be mechanisms defined to empower user to define his privacy and security requirements.

Hope Villiard et. al. [8] in a psychological study on effect of advertisements shown on Facebook profiles on the fitness of group of college students. They studied how much students discussed about fitness on Facebook platform and how this was linked to automatically generated advertisements for fitness products and advise. Study showed that information that people share such as status update etc. have direct linkage to advertisements that a person views. It was also noted that some of current advertisements being shown were not age appropriate or necessarily healthy. This gives scope for further improvement for kind of advertisements displayed to users. This is part of the concern that we raised when we asked question #2 related to advertisements.

Nour Mohammed Almadhoun[9] and Anil Dhami et. al.[10] have published their study on effect of privacy, trust and security concerns on willingness to share information and creating fresh relationships in social networking sites especially on Facebook. While former did its study on Malaysian higher education institutions' marketing, latter did survey of 250 Facebook users mostly between the age limit of

16-35 and having different national/cultural backgrounds. They were of opinion that trust had more impact on willingness to share information than privacy alone. However, this study model could be extented to identify key aspects with respects to specific age groups of specific national/cultural backgrounds.

Esma Aimeur et. al.[11], idetified three main privacy risks in social networks as Security, Credibility and Reputation & Profiling. A profile defining different levels of privacy settings has been proposed by them and end users can chose which one suits their purpose the most. Profiling solutions has been suggested by Varun M Deshpande et. al.[12] as well, along with need for customer driven Service Level Agreements

(SLAs) in cloud based systems. This helps in empowering end user to judiciously decide level of security. In Varun M Deshpande et. al. [13] discussed about a novel algorithm named Anveshana, for quality of service based ranking and selection algorithm. This algorithm which aims at directing user to the right service based on his requirements rather than the best available service. There may be applications of this algorithm in order to help user identify the best security as a service provider for them.

IV. RESEARCH DIRECTION

Literature review and the online survey have provided us with direction and helped us identify key areas where it is important to invest our efforts. In order to streamline the research focus, it is important to draw a boundary of our system and to identify the stakeholders of the same. In the broad paridgm of cloud computing, SaaS model would be of prime focus. Few of notable SaaS services such as social networking sites, email/messaging service providers, e-commerce websites would form the system for further research. Stakeholders include service providers, cloud data centers, end users, policy makers and law enforcement authorities, 3rd party beneficiearies like advertisers and data mining companies.

As directed by [11], [12], their exists scope of national/cultural secific studies encompassing different age groups and compare the results. This may help in identifying varied solutions based on user's background. We have identified 4 key aspects in which we would be directing our

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol4, Issue 6, June 2017

effort. They are trust, data security, privacy and policy driven We envison a system which has user centric design and customer could choose the level of security that is required as part of customer driven SLAs. Cloud service provider would provide an architecture that include privacy and data security profiles and increase the trust facrtor by increasing transperancy in data handling and related legislations.

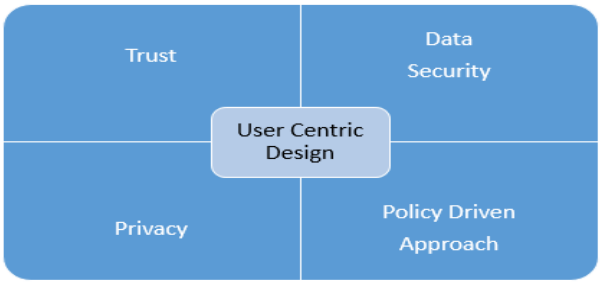


Figure 13: 4 Key Aspects of User Centric Design

Different countries have passed several legislations with respect to privacy and data security such as Health Insurance Portability and Accountability (HIPPA) act, HITEC act, PATRIOT act, Fedaral Information Security Management Act (FISMA) etc. in the U.S.A [2][14], Information Technology Act, Privacy Act etc. in India. We need to understand them in more detail which would help in developing better solutions for specific countries/regions. More research work is needed in identifying data deletion policies and also to understand what data is shared between service providers and advertisers when they generate advertisements based on user generated content.

• ***Trust***

It is a known fact that trust is built over a period of time and not an instantaneous process. In order to increase user's trust on cloud based services, several research directions can be envisioned. First of which is increasing transparency of how data is handled. Service providers may need to make architectural changes in order to realize Fail safe authentication mechanisms that ensure that data is secure even during an external hijack/attack on cloud servers. Authentication mechanisms ensuring that user accounts can never be stolen. Ex: using one time password authentication, better anonymization of user data before sharing it with 3rd party vendors, secure opt out mechanisms from personal data sharing.

• ***Privacy***

Level of privacy that users want, would vary from person to person. This is established by our online survey. Hence providing a mechanism where in user can choose level of privacy that he wants is of paramount importance. Many service providers have taken initiatives in order to achieve this objective. Still, there is a lot that can be done. Suppose, if a user doesn't want advertisements to be displayed or his information be sold to any 3rd party vendor; we need to identify ways in which this can be achieved in a way that is beneficial to both user and service provider. Also, there is a need for mechanisms through which user is able to understand how much of his own data is being leaked into public domain via social networking services. Once he knows about it, he should be able to judge and take informed decisions regarding privacy settings.

• ***Data Security***

There is a need for understanding data deletion policies and identifying key areas of improvement. This will help in resolving some of the concerns based on vendor lock-in issues. There is need for understanding encryption/session/cookie management of data being exchanged between client and server. Although this comes under web security domain, it can be considered part of current research work. There have been some vulnerabilities discovered recently such as Heart bleed bug. More research work is needed in identifying data deletion policies and to understand what data is shared between service providers and advertisers when they generate advertisements based on user generated content.

• ***Policy Driven***

Some of the policies related to privacy, trust and data security
in the current scenario of cloud computing are spread across multiple geos which have their own philosophies [16], [17]. This makes the topic highly complicated. We believe that an organized study of various policies of different countries must be done in a holistic manner to achieve continuously evolving, meaningful consensus across geos. Leading companies around the world who are one of the most prominent stake holders in this matter should play a very active role in driving these changes in the world. Currently, each company defines their own data policy. They have flexibility to define the rules of engagement with user's data. We believe that, this needs to be regulated using open standards on data security and privacy. Stakeholders from different areas such as security researchers, security companies, service providers, government regulatory
agencies and public need to sit together and arrive at uniform data sharing mechanisms and policies. These open standards need to be updated as per requirements in regular intervals.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol4, Issue 6, June 2017

V.TRUST BASED SECURE FRAMEWORK

A. Need for Holistic Data Policy Framework

Social Networking Services (SNS) such as Facebook and Google are reaping large amounts of revenue through advertising. They have a huge number of user base (about 2 billion monthly active users and well over 1 billion active daily users) and hence can reach out to high volume of users through their services. By defining their own privacy policy, they make it comfortable for them to make use of user generated data as per their requirements. Many of the privacy breaches are detected after the fact making it difficult to assess the potential damage done during privacy breach like improper usage of private or personally identifiable information. The current privacy guidelines defined across the globe have several short comings and lack technical correctness to enforce privacy protection at source. Other options such as ad-blockers don't solve the problem of data sharing between service provider and 3rd party. Hence, as security researchers, we need to understand the requirements from user perspective and propose privacy preserving data sharing mechanisms which will ensure business model
continuity and address the privacy and data security concerns of end users. We need to work towards setting up holistic technically feasible open standards with inputs from all stakeholders.

B. Problem Domain

In a system of SNS, the business model has these stakeholders (Fig 14): Service Providers such as Facebook or Google, Users who consume the product, advertisement frameworks such as Google AdSense, Facebook advertising framework which provide a platform for facilitating targeted advertising. Advertisers such as Amazon who want to advertise their products. Finally, data provider such as Acxiom, Datalogix which facilitate in analysis of user generated data and providing synthesized data.

Figure 14: SNS Stakeholders

With current work, we are trying to establish a regulated data policy framework to securely share the user generated data between service providers and other stake holders based on user preference. We need to empower the user to take

decisions regarding usage of the data. The data sharing policy framework needs to be transparent and adhering to open standards. While, providing means for user to securely opt out from sharing their information with 3rd party; framework should provide reasonable opportunities to service providers and other stake holders to sustain and grow their business. These solution needs to be technically correct and the
implementation done by the service provider needs to be verifiable. So that security companies could audit and certify the data contract policies in real time.

C. Open Standards for Data Sharing Policies

As part of the novel framework for secure data sharing policy, we propose that the policy management needs to happen through open standards. Open forum needs to be set up which includes representatives from leading security companies, security researchers, representations from various government agencies and service providers. This needs to be a global phenomenon handled by UN once the implementation of the framework becomes stabilized. To begin with, at least, we need to set standards within a country.

Open standards need to address factors such as what are the set of personal information which a service provider can collect or retain in database. How is the data collected and stored? Method of sharing data with 3rd party such as advertising frameworks. Data contract between service provider and 3rd party. Setting up secure protocols for data sharing. Providing means of securely opting out for the users who don't want to share data with 3rd party.

Varun M Deshpande et al.[18], described a method in order to provide a mechanism to securely opt out from personal data sharing between service provider and 3rd party. They showed how secure tokens can be used as a means of communication protocol for data sharing based on user preference. They tried to balance the requirement of user wanting not to share personal information and service providers need to generate revenue.

Once these open standards are standardized, they need to be followed by every service provider as part of a government

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol4, Issue 6, June 2017

regulation. Which makes it uniform law for all the service providers.

D. Policy Auditing and Certification Authority

In above section, we mentioned that the open standards would be applied to all service providers. We also mentioned that the standards should be technically correct and verifiable. Which means to say that we can infer precisely if a certain policy is currently implemented or not. The goal of auditing the service provider on a regular basis is to ensure that the open standards are adhered to as a process during change management. During course of product evolution, we should ensure that the open standards are not neglected or compromised.

We recommend that certification authorities need to be set up which will be entrusted with the certifying the service provider for adherence to standards which are set. Like the certification authorities – Verisign, Comodo etc. which certify the secure HTTPS transactions done to and from a website, the Policy auditing certifying authorities which show the proof of adherence and its logo on the website would mean that the end user can trust the service provider. Also, the framework should be implemented in such a way that the service providers without a valid certificate are marked as un secured and other websites and discouraged from communicating with them unless they are certified.

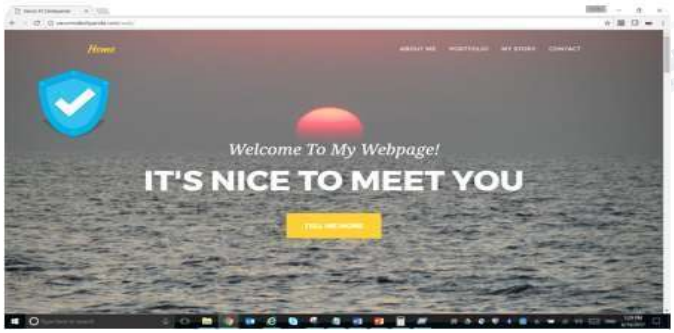


Figure 15: Website with Secure Logo from Cerification Authority (Representational image)

E. User Privacy Profiles and Premium Business Model

From the survey, we realize that there are various categories in user space which can be categories under different profiles. People who don't mind sharing their data if they get product choose is given to them. Hence, we advocate that we factor in flexible user profiles based on the context of the service provided in the data sharing policy. For example, we can have 3 user privacy profiles (fig 16) – Freemium, Standard and Premium. Each level would be costlier than the one below.

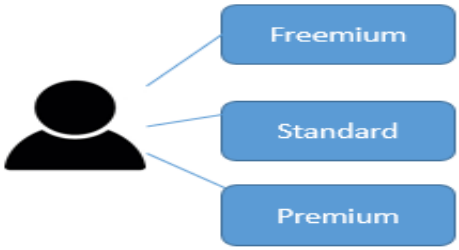


Figure 16: User Profiles

F. Design and Analysis of Secure Data Sharing Policy Framework

Below is a representational depiction of design of proposed data sharing policy framework. System boundary consists of components:

- Service Provider
- Advertisement Framework
- Advertisements
- Data Policy
- Certification Authority
- End Users

Data sharing between service provider, and other 3rd party is bound by the policy framework which is based on the agreed upon open standards for data sharing. User can choose one of the different user privacy profiles offered by service provider.

for free of service. However, there are studies done by researchers such as Micheal et al. [19] who share their results stating users are ready to pay a price to get enhanced privacy features. Their study highlighted group of people who were ready to pay up to 7.5 Euros a year for getting enhanced privacy features from a web site such as Facebook. Comparing it with latest Q1 2017 revenue of $24.7 Billion and about 2 billion monthly active users, Facebook in making about $1.2 per person per quarter with its freemium model. The net revenue per person per quarter would increase to over $2. This is close to 70% more revenue when compared to revenue from non-paying user.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol4, Issue 6, June 2017

So, this is profitable for the service provider.

We do recognize that there would be different privacy profiles to which people would choose to join, provided a chance to A certifying authority is responsible to audit the service provider for compliance with the set standards. Certificate from the certifying authority is displayed on the website with link to detailed reports that can be accessed on need basis. This certificate is a seal of trust that the users can bank upon. This framework would be common across all social networking and related online systems which deals with personal user information. This framework needs to be mandated from governing authorities to all the service providers in order maintain uniformity of policies and to give user a choice to choose the privacy profile that he is comfortable with. The open standards need to be updated timely manner and well documented. Web security related issues need to be taken into consideration and suitable measures need to be mandated.
The whole point of this exercise is to come up with technically feasible and transparent framework that would ensure that users can trust the service providers while interactive with digital world. By ensuring that all service providers are provided with new modes of generating revenue by adhering to open standards, we have struck a win-win deal for managing user privacy requirement and the business model continuity. Hence, this holistic approach has potential to be an ideal solution going forward.

VI.CONCLUSION AND FUTURE WORK

In this paper, we started with giving brief explanation of cloud computing as per NIST definitions. Major SaaS service providers in areas including social networking, mail/messaging services and e-commerce websites were discussed. We then spoke about our research domain that is concerned with digital privacy and data security for end users who use SaaS service offerings.

To understand this with an end user perspective, we reached out to public users of SaaS services. We asked them variety of questions to get a feel of level of trust and comfort users have when using SaaS service offering which are generally available at free of cost. Along with the survey, relevant literature survey was conducted and highlights were discussed in the paper. It is concurred that online digital identity is an important asset in current day life and managing it is an important task. Four key research areas – Trust, privacy, data security and policy driven approach have been identified.

Based on these 4 pillars, we proposed a trust based novel data sharing policy framework which tries to find technically feasible solution for data privacy related concerns in social networking. The solution put forth is a step towards developing trustable software solutions for secure cloud based solutions. By empowering both users by providing flexible user privacy profiles; and service providers by creating alternate revenue generating mechanism for collecting money from non-freemium users; we have established is Win-Win model which is poised for successful adoption.

Framework proposes to setup a dedicated team of security companies, service providers, government agencies and researchers for coming up with and maintaining open standards for personal data sharing between service providers and 3rd party. Certifying authorities would be setup to audit and certify the service providers for compliance with mandated data privacy regulations.

As part of future work, the specifics of contents of open standards and working of certifying authority needs to be developed and proposed. Also, evolution of data policies of notable companies such as Google and Facebook need to be understood and best practices and lessons carried forward.

REFERENCES

[1] Barrie Sosinsky, ―Cloud Computing Bible,‖ Published by John Wiley & Sons, 2011, J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.

[2] Ronald L. Krutz and Russel Dean Vines, ―Cloud Security: A Comprehensive Guide to Secure Cloud Computing,‖ Published by John Wiley & Sons, 2010

[3] Chi Zhang, Jinyuan Sun, Xiaoyan Zhu and Yuguang Fang, "Privacy and security for online social networks: challenges and opportunities" Published in IEEE Network Volume 24, Issue 4 in 2010, Pg 13-18

[4] Cutillo, L.A., Molva, R. and Strufe, T, "Privacy preserving social networking through decentralization", published in Wireless On- Demand Network Systems and Services, 2009. WONS 2009, IEEE, Pg 145-152

[5] Catherine Dwyer, Starr Roxanne Hiltz and Katia

Passerini, "Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace", Proceedings of the Thirteenth Americas Conference on Information Systems, Keystone, Colorado August 09 – 12 2007

[6] Elena Zheleva, Evimaria Terzi and Lise Getoor, "Privacy in Social Networks", Published by Morgan & Claypool Publishers in 2013

[7] G. Brown, T. Howe, M. Ihbe, A. Prakash, and K. Borders, "Social networks and context-aware spam.‖ In ACM Conference on Computer Supported Collaborative Work, 2008.

[8] Hope Villiard and Megan A. Moreno, "Fitness on Facebook: Advertisements Generated in Response to Profile Content", Published in Cyberpsychol Behav Soc Netw. Oct 2012; 15(10): 564–568.

[9] Nour Mohammed Almadhoun, P. dhanapal Darai Dominic and Lai Fong Woon, "Perceived Security, Privacy and Trust concerns within Social Networking Sites" ,Published in IEEE International Conference on Control System,, Computing and Engineering in 2011

[10] Anil Dhami, Neha Agarwal, Tamal Chakraborthy, Brijendra Pratap Singh and Jasmine Minj, "Impact of trust, security and privacy concerns in social networking: An exploratory study to understand the pattern of information revelation in Facebook", Published in 3rd IEEE International Advance Computing Conference, 2013.

[11] Esma Aimeur, Sebastian Grams and Ai Ho, ―Towards a Privacy- enhanced Social Networking Site‖, Published in International Conference on Availability , Reliability and Security, 2010.

[12] Varun M Deshpande, Dr. Mydhili K. Nair, Balaji Soundararajan(2013), Customer Driven SLA in Cloud Based Systems, In Proceedings published by Elsevier of International Conference of Emerging Computations and Information Technologies, SIT, Tumkur, Karnataka (India), 22-23 November, 2013, pp 508-518

[13] Varun M Deshpande, Dr. Mydhili K. Nair (2014), Anveshana – Search for the Right Service, In Proceedings published by IEEE of International Conference of Convergence of Technology, Pune, Maharastra (India), ISBN 978-1-4799-3759-2

[14] Mark Rhodes-Ousley, "Information Security The Complete Reference, Second Edition", Published by Tata McGraw-Hill, 2013

[15] Online Survey on Digital Privacy, Resultshttps://docs.google.com/spreadsheets/d/1WqD5_AomCdnTlNS_SmEkX yXbNJ6QnepcsaPuOJAzT-Y/edit#gid=1319521219

[16http://ec.europa.eu/justice/dataprotection/individuals/index_en.htm(Last Accessed on Feb 18, 2016)

[17]http://www.it.ojp.gov/PrivacyLiberty/authorities/statutes/1287 (Last Accessed on Feb 18, 2016)

[18] Varun M Deshpande, Dr. Mydhili K. Nair (2017), ―A Novel Framework for Privacy Preserving Ad-Free Social Networking‖, published in Proceedings by IEEE of 2017 2nd International Conference for Convergence in Technology (I2CT), Pune, Maharastra (India), ISBN 978-1-5090-4307-1/17

[19] Michel Schreiner, Thomas Hess,2015 "WHY ARE CONSUMERS WILLING TO PAY FOR PRIVACY?AN APPLICATION OF THE PRIVACY-FREEMIUM MODEL TO MEDIA COMPANIES" published in Twenty-Third European Conference on Information Systems (ECIS), Münster, Germany, 2015